IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	PETROGIANNIS et al.	Examiner:	William S. Powers
Serial No.:	10/022,559	Group Art Unit:	2134
Filed:	December 14, 2001	Docket No.:	09680.0188USU1
Customer No.	23552	Confirmation No.	3770
Title:	WEB-BASED METHOD AND SYSTEM FOR APPLYING A LEGALLY ENFORCEABLE SIGNATURE ON AN ELECTRONIC DOCUMENT		

APPELLANTS' BRIEF ON APPEAL

Mail Stop APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Brief is presented in support of the Notice of Appeal filed November 18, 2009, from the final rejection of claims 1-12, 14, 17-36, 38, 41-59 and 63-68 of the above-identified application, as set forth in the Final Office Action mailed October 20, 2008 and Non-Final Office Action mailed June 18, 2009.

Payment is made by credit card in the amount of $270.00 to cover the required fee for a small entity.

An oral hearing is requested. A separate request for oral hearing with the appropriate fee will be filed within two months of the Examiner's Answer.

I. REAL PARTY OF INTEREST

The real party of interest is Silanis Technology, Inc. of St-Laurent, Quebec, Canada, by way of assignment recorded on March 25, 2002 at Reel 012751 and Frame 0415.

II. RELATED APPEALS AND INTERFERENCES

There are no currently pending related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-12, 14, 17-36, 38, 41-59 and 63-68 are pending. Claims 1-12, 14, 17-36, 38, 41-59 and 63-68 have been rejected and are the subject of the appeal. Claims 13, 15-16, 37, 39-40 and 60-62 have been cancelled without prejudice or disclaimer. All pending claims are listed in the Claims Appendix that follows.

Claims 1, 2, 4-6, 8-12, 14, 17, 22-27, 29, 30, 32-36, 38, 41, 46-50, 52-55, 57-59, 63, 67 and 68 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication 2001/0014839 to Belanger et al. in combination with U.S. Patent No. 6,091,835 to Smithies et al., U.S. Patent No. 7,209,571 to Davis et al. and U.S. Patent No. 6,085,322 to Romney et al.

Claims 3, 31 and 51 stand rejected as being unpatentable over U.S. Patent Application Publication 2001/0014839 to Belanger et al. in combination with U.S. Patent No. 6,091,835 to Smithies et al., U.S. Patent No. 7,209,571 to Davis et al. and U.S. Patent No. 6,085,322 to Romney et al.

Claim 7, 28 and 56 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication 2001/0014839 to Belanger et al. in combination with U.S. Patent No. 6,091,835 to Smithies et al., U.S. Patent No. 7,209,571 to Davis et al., U.S. Patent No. 6,085,322 to Romney et al. and U.S. Patent No. 6,151,624 to Teare et al.

Claims 18-21, 42-45 and 64-66 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication 2001/0014839 to Belanger et al. in combination with U.S. Patent No. 6,091,835 to Smithies et al., U.S. Patent No. 7,209,571 to Davis et al., U.S. Patent No. 6,085,322 to Romney et al. and U.S. Patent No. 5,606,609 to Houser et al.

IV. STATUS OF AMENDMENTS

No amendments were filed after the Office Action of June 18, 2009.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

A summary of the claimed invention follows. The summary includes references to an embodiment disclosed in the specification.

Independent claim 1 recites a web based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment. See page 4, lines 27-30 and page 5, lines 18-20. Claim 1 further recites the steps of having the user access the web environment through a web browser to a secure electronic system, said electronic system having verified the identity of the user. See page 5, lines 8-10; page 5, lines 23-27; page 9, lines 15-16; page 11, line 26 to page 12, line 2 and Figure 1. Claim 1 further recites having the user sign the electronic document in said web environment. See page 9, line 17. Further, said signing comprises modules on the server performing substeps. See page 5, lines 15-18. The substeps include presenting the user with a web-based representation of the document in said web browser. See page 6, lines 5-8 and 12-13; page 9, lines 20-22; and page 12, lines 28-30. Claim 1 further recites presenting the user with legal information related to said signing, and getting agreement from the user of said legal information in said web browser. See page 6, lines 20-25; page 7, lines 1-6; page 9, lines 23-26; page 12, lines 13-19; page 13, lines 6-9 and Figure 1. Finally, the substeps include upon agreement of the legal information from the user, applying said signature of the user on said document on the server. See page 7, lines 8-19; and page 9, line 27 to page 10, line 3. Claim 1 also recites on the server, generating a process log of the signing. See page 7, line 21. Said process log comprises a record of the substeps as executed and allows reconstruction with the web-based representation of the document of the legal information as presented to the user through the said web browser. See page 7, lines 28-30; page 9, lines 4-6 and Figure 3. Claim 1 further recites securely associating said process log with the document as signed. See page 7, line 22 and page 8, lines 1-3. Claim 1 recites that the securely associating comprises a substep of generating a secure process authentication code uniquely representing the process log, said

secure process authentication code being a hash of said process log. See page 8, lines 3-6 and Figure 1; and page 9, lines 6-8 and Figure 3. The securely comprising includes the additional substep of embedding said process authentication code in said document as signed, thereby securely associating said process log and the document. See page 8, lines 3-6; and page 9, line 8. Finally, claim 1 recites making the document as signed available to the user. See page 9, lines 9-11 and Figure 3.

Independent claim 25 recites a web-based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment. See page 4, lines 27-30; and page 5, lines 18-20 and Figure 1. The method comprises having the user access the web environment through a web browser from a secure electronic system, said secure system having verified an identity of the user. See page 5, lines 8-10 and 23-27; page 9, lines 15-16; page 11, line 26 to page 12, line 2 and Figures 1-3. Claim 1 further recites having the user sign the electronic document in said web environment. See page 9, line 17. Said signing comprising modules on the server performing sub steps. See page 5, lines 15-18. Claim 1 recites the substeps of presenting the user with legal information related to said signing, in getting agreement from the user of said legal information in said web browser. See page 6, lines 20-25; page 7, lines 1-6; page 9, lines 23-26; page 12, lines 13-19 and page 13, lines 6-9. Claim 1 recites the additional substep of presenting the user with a web-based representation of the document information in said web browser. See page 6, lines 20-25, page 7, lines 1-6; page 9, lines 23-26; page 12, lines 15-19; and page 13, lines 6-9. Claim 25 recites the additional substep of getting confirmation from the user that the document is to be signed through said web browser. See page 6, lines 17-19. Claim 1 further recites the substep of applying said signature of the user on said document on the server. See page 7, lines 8-19. In addition, claim 25 recites generating a process log of the signing step on the server. See page 7, line 21. The process log comprising the executed substeps and allowing reconstruction of the web-based representation of the document and of the legal information as presented to the user through the web browser. See page 7, lines 28-30; and page 9, lines 4-6. Claim 25 also recites

securely associating said process log with the document to sign. See page 7, lines 22-24; and page 8, lines 1-3. Said securely associating comprises the substep of generating a secure process authentication code uniquely representing said process log, said secure process authentication code being a hash of said process log. See page 8, lines 3-6; and page 9, lines 6-8. Claim 25 also recites the substep for the associating comprising embedding said process authentication code in said document to sign, thereby securely associating said process log and document. See page 8, lines 3-6; and page 9, line 8. Finally, claim 25 recites making the document as signed available to the user. See page 9, lines 9-11.

Independent claim 49 recites a system for applying a legally-enforceable signature of a user on an electronic document in a web environment, an electronic document located on a server. See page 4, lines 27-30; page 5, lines 13-20 and Figure 1. Said system comprises accessing means for accessing said web environment from the secure electronic system through a web browser. See page 5, line 21 to page 6, line 4. Claim 49 further recites a document-rendering module on the server for presenting the user with a web-based representation of said document in said web browser. See page 6, lines 5-19. Claim 49 also recites a legal disclosure module on the server for presenting the user, and said web browser, with legal information related to electronically signing said document, for obtaining agreement from the user of said legal information document in said web browser. See page 6, line 20 to page 7, line 6. Claim 49 also includes a document approval module on the server for providing the signature of the user to the document upon agreement from the user of the legal information, thereby signing said document. See page 7, lines 7-19. Claim 49 further includes a process log module on the server for generating the process log of the signing of the document and securely associating said process log with the document to sign. See page 7, lines 20-22. Said process log comprises reconstruction data for allowing the reconstruction of the presenting the user with said web-based representation of the document, of said presenting the user with said legal information, and of said obtaining agreement from the user of said legal information and of said signing of the document. See page 7, lines 22-30. Claim 49 further recites said process log module comprising

means for generating the secure process authentication code uniquely representing said process log, and embedding said secure process authentication code in said document to sign, thereby securely associating said process log and document, said means to generate a secure process authentication code comprising a hash module. See page 8, lines 1-12. Claim 49 also includes a document distribution module for making the document as signed available to the user. See page 8, lines 13-22. Finally, claim 49 recites that said accessing means and said document-rendering, legal disclosure, document approval, process log and document distribution modules are server based. See page 4, line 31 to page 5, line 2; page 5, lines 18-20 and Figure 1.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4, 5, 6, 8-12, 14, 17, 22-27, 29, 30, 32-36, 38, 41, 46-50, 52-55, 57-59, 63, 67 and 68 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Application Publication 2001/0014839 to Belanger et al., in view of U.S. Patent No. 6,091,835 to Smithies et al., in view of U.S. Patent No. 7,209,571 to Davis et al., and further in view of U.S. Patent No. 6,085,322 to Romney et al.

Whether claims 3, 31 and 51 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Application Publication 2001/0014839 to Belanger et al., in view of U.S. Patent No. 6,091,835 to Smithies et al., in view of U.S. Patent No. 7,209,571 to Davis et al., in further view of U.S. Patent No. 6,085,322 to Romney et al., and further in view of U.S. Patent No. 5,649,186 to Ferguson.

Whether claims 7, 28 and 56 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Application Publication 2001/0014839 to Belanger et al., in view of U.S. Patent No. 6,091,835 to Smithies et al., in view of U.S. Patent No. 7,209,571 to Davis et al., in further view of U.S. Patent No. 6,085,322 to Romney et al., and further in view of U.S. Patent No. 6,151,624 to Teare et al.

Whether claims 18-21, 42-45 and 64-66 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Application Publication 2001/0014839 to Belanger et al., in view of U.S. Patent No. 6,091,835 to Smithies et al., in view of U.S. Patent No, 72,09,571 to Davis et al., in further view of U.S. Patent No. 6,085,322 to Romney et al., and further in view of U.S. Patent No. 5,606,609 to Houser et al.

VII. ARGUMENT

Claims 1, 2, 4, 5, 6, 8-12, 14, 17, 22-27, 29, 30, 32-36, 38, 41, 46-50, 52-55, 57-59, 63, 67 and 68, including independent claims 1, 25 and 49, stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Belanger, Smithies, Davis and Romney. Applicants respectfully assert that the position taken by the Examiner is in error. Applicants accordingly appeal the rejection of these claims rejected under 35 U.S.C. § 103(a) being unpatentable over Belanger, Smithies, Davis and Romney. Applicants present herein below particular errors made in the rejection of these claims.

Independent Claim 1

Independent claim 1 generally relates to a method providing for the application of a legally enforceable signature on an electronic document in a web environment. The electronic document is located on a server and the user interacts with the web environment through a web browser. The server has multiple modules that control the presentation of the document to the user, as well as controlling the signing ceremony and controlling the logging processes. The method of the present invention provides advantages by allowing the user to perform the signing ceremony solely through the use of the web browser, without the need for installation of special software on the user's computer system. The signer's intent and acceptance forming a legal agreement is reproducible at a later time as the web pages that are presented to the user through the browser and the user's actions in moving from one web page to another are recorded in a process log that allows the reconstruction of the entire presentation of web pages to the user, including the contents of the documents and the actions taken by the user in moving from web page to web page while reviewing the documents. The collective features recited in claim 1 interact together in a new, novel and non-obvious way to obtain an advantageous method.

The Office Action states that Belanger teaches steps that are admittedly known in the

prior art. Belanger teaches having the user access the web environment through a web browser from a secure electronic system that has verified the identity of the user and having the user sign the electronic document in the web environment. The Office Action also states that the system of Belanger resides on the internet server and that the user only needs a computing device with a web browser to use all the functions of the system. In addition, the Office Action states that Belanger further teaches the application of digital signatures and the creation and manipulation of electronic documents. See paragraphs 31 and 35 of the published Belanger application. Applicants do not concede the correctness of these contentions.

However, Applicants note that the Office Action does not provide arguments regarding several limitations to the claim or demonstrate that Belanger teaches the steps. The Office Action is silent as to Belanger presenting the user with a web based representation of the document in the browser and presenting the user with legal information related to the signing, getting agreement from the user of the legal information in the web browser and upon agreement of the legal information from the user, applying the signature of the user on the document on the server. In addition, Applicants assert that step c) is not shown or suggested by Belanger in the Office Action. Step c) recites on the server, generating a process log of the signing of step b), said process log comprising a record of substeps b(i) – b(iii) as executed in allowing the reconstruction of web based representation of the document and the legal information as presented to the user through the web browser.

The Office Action then relies on Smithies to demonstrate that the steps not shown or suggested by Belanger would be known to one skilled in the art. Applicants respectfully disagree that these steps are shown or suggested by Smithies. Applicants note that the arguments were raised in the Amendment filed on April 20, 2009. Applicants reiterate these arguments and assert that the arguments have not been fully considered and that no reason has been provided why the arguments are not persuasive. Moreover, the Action has not refuted the arguments raised in the Amendment of April 20, 2009.

Applicants assert that the first substep b(i) of claim 1, includes presenting the user with a web-based representation of the document in the web browser. As explained in the specification, in practice this may be realized, for example, by a merchant e-commerce website performing a hand-off to the e-Signing Process (the server) and providing all the necessary data and information to generate the appropriate contract for approval and signature. In the method recited in claim 1, the server therefore manages the signing ceremony and presents the document through a web browser to the user rather than the merchant or another system or application.

The Office Action refers to Smithies at column 42, lines 8-24, to support that this step is known from the prior art. However, the step is not shown. In Smithies, the presentation of web pages to the affirming party is one process performed by one system while the signing ceremony is a different process performed by a different system. The information relating to the form to sign is presented to the affirming party by the Web Server in Smithies, see column 42, line 22. However, the interactions with the affirming party that make up the signing ceremony are managed by the transcript generator module. See column 42, lines 32-36 of Smithies.

Moreover, the substep b(ii) of claim 1 relates to presenting the user with legal information concerning the signing and obtaining the user's agreement with this information in the web browser. The Examiner relies on Smithies at column 34, lines 8-17, to argue that the step is known in the prior art. Although this passage refers to the presenting of information related to a legal issue, legal accountability to an affirming party, the passage does not teach or suggest that this should be done through a web browser. Moreover, the passage does not teach or suggest that the user's interaction with the web browser would be used to obtain the agreement with legal information. The present application describes embodiments may be achieved by providing "I Agree" buttons or equivalents in the relevant web pages. As the particular embodiment described in the cited passage of Smithies is not carried out in a web environment, the use of a web browser in this context cannot be inferred from the passage. In a web embodiment of Smithies described in columns 41-42, the presenting and agreement of legal

information is not discussed or mentioned. Applicants further note that in the web embodiment of Smithies, an interface program is installed on the user's computer system to interact with the affirming party. In addition, Smithies does not rely on the web pages presented to the user containing the form in order to interact with the user and create the signing ceremony. Applicants therefore assert that Smithies cannot teach a step of "presenting the user with legal information related to said signing, and getting agreement from the user of said legal information **in said web browser**." (Emphasis added).

In substep b(iii) of claim 1, upon obtaining the signing command and agreement of the legal information from the user, the signature of the user is applied to the document on the server. The Office Action cites column 34 line 61 – column 35 line 49 of Smithies to show that this step is known. However, the cited passage does not discuss or mention in any way the actual application of the signature on the document. Moreover, the cited passage does not discuss or teach that the document resides on a server. The server-related aspect of claim 1 cannot be demonstrated by the embodiment of the passage cited in Smithies as actions do not take place over the web. Moreover, in the only web embodiment of Smithies, the document does not reside on the server performing the signing ceremony. In Smithies, the document is a web form presented to the affirming party by a different entity than the transcript generator module managing the ceremony. As the signature is never sent to that entity in Smithies, the signature cannot be applied to the document at all. Therefore it is clear that Smithies does not teach all of the features of substep b(iii).

Turning now to step c) of claim 1, a process log of the signing of step b) is generated on the server. The process log comprises a record of the substeps b(i) to b(iii) as executed, and provides for reconstruction of the web-based representation of the document and of the legal information as presented to the user through the web browser. The Office Action contends that "....transcript object recreates the documents and **all actions during the signing procedure** to the user for final approval of the signature and document (See Smithies, column 42, lines 32-

52)". See page 7 of the Office Action. However, close scrutiny shows that column 42, lines 32-52 of Smithies states that the transcript object stores all the interactions between the affirming party in a small window generated by the interface program invoked by the transcript generator module. However, these interactions cannot include the web-based representation of the document being affirmed as presented to the user, since this document is never presented in the window in question. The presenting of the document "the form" being affirmed actually performed by the website embodying the client application and **not** by the transcript generator module. See Smithies, column 42, lines 22-30. The transcript generator module cannot keep a record of the step of "presenting the user with a web-based representation of the document in said web browser" as the transcript generator module is not involved in this step and does not possess the relevant information. Although this is logical in the context of the invention of Smithies, the claimed transcript generator module of Smithies is designed to be independent from the object being affirmed to preserve versatility. Therefore, the transcript generator module can be used in conjunction with a variety of applications such word processing programs, spreadsheet programs, or specialized software, to perform or record the occurrence of an event in which the affirming party participates. See column 12, lines 3-27 of Smithies.

Moreover, Smithies does not consider having a same entity, the server, handle the presentation of the document to be affirmed, the steps of the signing ceremony, and the generation of the process log as Smithies promotes the segregation of these tasks among different components to prevent forgery. See column 9, lines 45-54 of Smithies. In addition, at paragraph 3 of the Office Action, the contention is made that the Applicants have limited their arguments only to specific passages cited by the Examiner. Applicants respectfully disagree. Although Applicants appreciate that the cited references are to be considered as a whole, Applicants assert that one will also appreciate that Applicants are responding to the contentions of a particular cited passage and that response must be made at a minimum to the characterization and application of the teaching of the particular passages. Moreover, although the cited passages of

Smithies have been used as a natural starting point to demonstrate the errors in reasoning on which the rejections of the present claims are based, other relevant passages are also addressed. Applicants note that they have identified particular embodiments and teachings of Smithies that are not necessarily cited. For example, Applicants have addressed the only web embodiment of Smithies. Applicants further note that the prosecution history of this application is lengthy. Applicants have carefully reviewed all of the teachings of Smithies on more than one occasion and have endeavored to fully comprehend the systems described in the context of the entire specification, rather than only the cited passages. Applicants therefore assert that Smithies as a whole fails to teach or suggest all passages of claim 1 for which it is relied upon when carefully reviewed as discussed above.

Applicants further assert that in the method of claim 1 of the present application, the interaction with the user is recorded indirectly. In claim 1, only the web pages presented to the user, including the web-based representation of the document to be signed, need to be included in the process log. The record of the signing ceremony follows from the contents and logic of the presentation of the particular web pages. Therefore, it can be seen that the fact that the user saw a particular web page signifies that he previously clicked on the appropriate button and therefore gave the signing command or indicated approval of the legal information presented in a previous web page. The content of each web page presented to the user and the order of the web pages, demonstrate the entire process. This allows the process log to provide evidence of the signing ceremony without the need to interact directly with the user's computer system, such as through an interface program like the Java applet of the web embodiment of Smithies. Moreover, the present invention provides a simple and elegant manner of keeping a full record of the transaction without having to directly record every interaction of the affirming party with the system, as must be done with Smithies.

Moreover, Smithies is representative of the general view of those skilled in the art prior to the present invention. The general view held that in order to provide a proper record of the

signing ceremony of a document online, it was necessary to collect data related to the interaction of the user with the signing software while the viewing of the document, transaction or event being affirmed, was controlled by a different process. Conversely, the invention as recited in claim 1 presents a significant departure from this view as the present invention relies on the logic of the web pages presented to the user, including the document or information being affirmed or signed to provide a record of the signing ceremony. The contents of the record reveal all of the information that has been presented to the user, and not just the steps in which the user has responded to this information. The approach of the present invention provides a significant advantage in a web environment as a server and any associated logic or programming presents requested web pages by creating them only as required for a particular user at a given moment. This does not store those particular pages as presented as a single record. Applicants assert that it would therefore be extremely difficult to reproduce the web pages presented to a user at a given time. Applicants assert that none of the cited prior art, including Smithies, Belanger or any other cited reference or combination teach or suggest such an approach, strategy or process. Applicants therefore assert that claim 1 patentably distinguishes over the prior art and requests that the rejection be withdrawn.

Applicants note that in addition to Belanger and Smithies, the other cited prior art or any other known prior art, fails to remedy the shortcomings of Belanger and Smithies. Applicants therefore assert that the prior art or any combination thereof fails to establish a *prima facie* case of obviousness.

Moreover, Applicants assert that independent claims 25 and 49 also patentably distinguish over the prior art for at least similar reasons. Applicants also assert that the dependent claims are also allowable for their dependence upon the allowable independent claims. Applicants therefore assert that the rejections under 35 U.S.C. § 103(a) must be withdrawn.

SUMMARY

In summary, Applicants assert that claims 1, 25 and 49 and the claims depending thereon, patentably distinguish over the prior art. Applicants therefore request that the rejections under 35 U.S.C. § 103(a) be withdrawn and that the Appeal be granted.

A speedy and favorable action in the form of a Notice of Allowance is hereby solicited. If the Examiner feels that a telephone interview may be helpful in this matter, please contact Applicant's representative at (612) 336-4728.

Please consider this a PETITION FOR EXTENSION OF TIME for a sufficient number of months to enter these papers or any future reply, if appropriate. Please charge any additional fees or credit overpayment to Deposit Account No. 13-2725.

Respectfully submitted,

MERCHANT & GOULD P.C.

Dated: 4/19/10

By: _____
Gregory A. Sebald
Reg. No. 33,280
GAS/krn

VIII. CLAIMS APPENDIX

1. A web-based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment, said method comprising the steps of:

a) having the user access the web environment through a web browser from a secure electronic system, said secure system having verified the identity of the user;

b) having the user sign the electronic document in said web environment, said signing comprising modules on the server performing the substeps of:

i) presenting the user with a web-based representation of the document in said web browser;

ii) presenting the user with legal information related to said signing, and getting agreement from the user of said legal information in said web browser; and

iii) upon agreement of the legal information from the user, applying said signature of the user on said document on the server;

c) on the server, generating a process log of the signing of step b), said process log comprising a record of substeps b) i) to b) iii) as executed and allowing the reconstruction of the web-based representation of the document and of the legal information as presented to the user through said web browser, and securely associating said process log with the document as signed, said securely associating comprising the substeps of:

i) generating a secure process authentication code uniquely representing said process log, said secure process authentication code being a hash of said process log; and

ii) embedding said process authentication code in said document as signed, thereby securely associating said process log and document; and

d) making the document as signed available to the user.

2. A method according to claim 1, wherein substep b) i) comprises retrieving said document from a document storing location.

3. A method according to claim 1, wherein substep b) i) comprises generating said document from a template.

4. A method according to claim 1, wherein substep b) i) comprises transforming said document from a non-web format to a web-format.

5. A method according to claim 1, wherein, in step b) ii), said legal information comprises information about legal implications of the signing of the document.

6. A method according to claim 1, wherein, in step b) ii), said legal information comprises legal disclosures related to said document.

7. A method according to claim 1, wherein substep b) ii) comprises presenting said legal information in a series of web pages.

8. A method according to claim 1, wherein substep b) ii) comprises presenting said legal information in a series of dialog boxes.

9. A method according to claim 1, wherein substep b) iii) comprises associating user-specific information to said document.

10. A method according to claim 9, wherein, in substep b) iii), said user-specific information is included in a special signature file defining the signature of the user.

11. A method according to claim 9, wherein substep b) iii) further comprises associating a digital certificate and private key to the document.

12. A method according to claim 9, wherein substep b) iii) further comprises obtaining said user-specific information from the secure electronic system.

13. (CANCELLED)

14. A method according to claim 1, wherein step c) further comprises storing said process log in a log database.

15-16. (CANCELLED)

17. A method according to claim 1, comprising an additional step before step d) of providing an audit trail of the signing of step b) in the document as signed.

18. A method according to claim 17, wherein said additional step comprises including a secure document authentication code uniquely representing said document as signed in said audit trail.

19. A method according to claim 18, wherein said additional step further comprises storing said secure document authentication code in a database.

20. A method according to claim 18, wherein said additional step further comprises generating a hash of said document as signed defining the secure document authentication code.

21. A method according to claim 1, comprising an additional step before step d) of embedding a secure document authentication code uniquely representing the document as signed inside said document.

22. A method according to claim 1, wherein step d) comprises transmitting a copy of the document as signed to the user.

23. A method according to claim 1, wherein step d) comprises enabling the user to download the document as signed.

24. A method according to claim 1, wherein step d) further comprises making the document as signed available to at least one additional party concerned by said electronic document.

25. A web-based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment, said method comprising the steps of:

a) having the user access the web environment through a web browser from a secure electronic system, said secure system having verified an identity of the user;

b) having the user sign the electronic document in said web environment, said signing comprising modules on the server performing the substeps of:

i) presenting the user with legal information related to said signing, and getting agreement from the user of said legal information in said web browser;

ii) presenting the user with a web-based representation of the document information in said web browser;

iii) getting confirmation from the user that the document is to be signed information through said web browser; and

iv) applying said signature of the user on said document on the server;

c) on the server, generating a process log of the signing of step b), said process log comprising a record of substeps b) i) to b) iv) as executed and allowing the reconstruction of the web-based representation of the document and of the legal information as presented to the user through said web browser, and securely associating said process log with the document as signed, said securely associating comprising the substeps of:

i) generating a secure process authentication code uniquely representing said process log, said secure process authentication code being a hash of said process log; and

ii) embedding said process authentication code in said document as signed, thereby securely associating said process log and document; and

d) making the document as signed available to the user.

26. A method according to claim 25, wherein, in step b) i), said legal information comprises information about legal implications of the signing of the document.

27. A method according to claim 25, wherein, in step b) i), said legal information comprises legal disclosures related to said document.

28. A method according to claim 25, wherein substep b) i) comprises presenting said legal information in a series of web pages.

29. A method according to claim 25, wherein substep b) i) comprises presenting said legal information in a series of dialog boxes.

30. A method according to claim 25, wherein substep b) ii) comprises retrieving said document from a document storing location.

31. A method according to claim 25, wherein substep b) ii) comprises generating said document from a template.

32. A method according to claim 25, wherein substep b) ii) comprises transforming said document from a non-web format to a web-format.

33. A method according to claim 25, wherein substep b) iv) comprises associating user-specific information to said document.

34. A method according to claim 33, wherein, in substep b) iv), said user-specific information is included in a special signature file defining the signature of the user.

35. A method according to claim 33, wherein substep b) iv) further comprises associating a digital certificate and private key to the document.

36. A method according to claim 33, wherein substep b) iv) further comprises obtaining said user-specific information from the secure electronic system.

37. (CANCELLED)

38. A method according to claim 25, wherein step c) further comprises storing said process log in a log database.

39-40. (CANCELLED)

41. A method according to claim 25, comprising an additional step before step d) of providing an audit trail of the signing of step b) in the document as signed.

42. A method according to claim 41, wherein said additional step comprises including a secure document authentication code uniquely representing said document as signed in said audit trail.

43. A method according to claim 42, wherein said additional step further comprises storing said secure document authentication code in a database.

44. A method according to claim 42, wherein said additional step further comprises generating a hash of said document as signed defining the secure document authentication code.

45. A method according to claim 25, comprising an additional step before step d) of embedding a secure document authentication code uniquely representing the document as signed inside said document.

46. A method according to claim 25, wherein step d) comprises transmitting a copy of the document as signed to the user.

47. A method according to claim 25, wherein step d) comprises enabling the user to download the document as signed.

48. A method according to claim 25, wherein step d) further comprises sending a copy of the document as signed to at least one additional party concerned by said electronic document.

49. A system for applying a legally-enforceable signature of a user on an electronic document in a web environment, the electronic document located on a server, said system comprising:

accessing means for accessing said web environment from a secure electronic system through a web browser;

a document-rendering module on the server for presenting the user with a web-based representation of said document in said web browser;

a legal disclosure module on the server for presenting the user, in said web browser, with legal information related to electronically signing said document, and for obtaining agreement from the user of said legal information document in said web browser;

a document approval module on the server for providing the signature of the user to the document upon agreement from the user of the legal information, thereby signing said document;

a process log module on the server for generating a process log of the signing of the document and securely associating said process log with the document as signed, said process log comprising reconstruction data for allowing the reconstruction of the presenting the user with said web-based representation of the document, of said presenting the user with said legal information, of said obtaining agreement from the user of said legal information and of said signing of the document, said process log module comprising means for generating a secure process authentication code uniquely representing said process log, and embedding said secure process authentication code in said document as signed, thereby securely associating said process

log and document, wherein said means to generate a secure process authentication code comprise a hash module; and

a document distribution module for making the document as signed available to the user,

wherein said accessing means and said document-rendering, legal disclosure, document approval, process log and document distribution modules are server-based.

50. A system according to claim 49, wherein said document-rendering module comprises retrieving means for retrieving said document from a document storing location.

51. A system according to claim 49, further comprising a document customization module cooperating with the document-rendering module for generating said document from a template.

52. A system according to claim 49, wherein said document-rendering module comprises transforming means for transforming said document from a non-web format to a web-format.

53. A system according to claim 49, wherein said legal information comprises information about legal implications of the signing of the document.

54. A system according to claim 49, wherein said legal information comprises legal disclosures related to said document.

55. A system according to claim 49, wherein said legal disclosure module comprises displaying means for displaying said legal information in a web-based medium.

56. A system according to claim 55, wherein said web-based medium includes a plurality of web pages.

57. A system according to claim 55, wherein said web-based medium includes a plurality of dialogue boxes.

58. A system according to claim 49, further comprising a user binding module cooperating with the secure electronic system to obtain therefrom user-specific information, generating a special signature file using said user-specific information and providing said special signature file to the document approval module, said special signature file defining the signature of the user.

59. A system according to claim 58, wherein said user-specific information comprises a digital certificate and private key.

60-62. (CANCELLED)

63. A system according to claim 49, further comprising an audit trail module for providing an audit trail of the signing of the document in said document as signed.

64. A system according to claim 63, wherein said audit trail includes a secure document authentication code uniquely representing said document as signed.

65. A system according to claim 64, wherein the document authentication code is a hash of said document as signed.

66. A system according to claim 49, wherein the document approval module comprises means for embedding a document authentication code uniquely representing the document as signed inside said document.

67. A system according to claim 49, wherein said document distribution module comprises means for transmitting a copy of the document as signed to the user.

68. A system according to claim 69, wherein said document distribution module provides a copy of the document as signed to at least one additional party concerned by said electronic document.

IX. EVIDENCE APPENDIX

A. OFFICE ACTIONS AND AMENDMENTS/RESPONSES

1. Office Action dated July 14, 2005
2. Amendment filed January 17, 2006.
3. Final Office Action dated April 14, 2006.
4. Amendment filed October 13, 2006.
5. Office Action dated November 28, 2006.
6. Amendment filed May 29, 2007.
7. Final Office Action dated August 13, 2007.
8. Amendment filed October 31, 2007.
9. Office Action dated January 31, 2008.
10. Amendment filed July 31, 2008.
11. Final Office Action dated October 20, 2008.
12. Amendment filed April 20, 2009.
13. Office Action dated June 18, 2009.
14. Notice of Appeal filed November 18, 2009.

B. REFERENCES RELIED UPON BY THE EXAMINER

1. U.S. Patent Application Publication 2001/0014839 to Belanger et al.;
2. U.S. Patent No. 6,091,835 to Smithies et al.;
3. U.S. Patent No. 7,209,571 to Davis et al.;
4. U.S. Patent No. 6,085,322 to Romney et al.;
5. U.S. Patent No. 5,649,186 to Ferguson;
6. U.S. Patent No. 6,151,624 to Teare et al.; and
7. U.S. Patent No. 5,606,609 to Houser et al.

C. REFERENCES CITED BY APPELLANTS

None.

D. CASES CITED IN THE BRIEF

None.

X. RELATED PROCEEDINGS APPENDIX

None.